Réinitialisation du mot de passe FTD du pare-feu sécurisé ; Après perte du mot de passe

Problème

Firewall Threat Defense (FTD) est devenu inaccessible via l'interface de ligne de commande en raison d'un mot de passe administrateur local perdu. Impossible d'accéder au noeud affecté à des fins administratives. L'hypothèse initiale était que le mot de passe d'administrateur avait été modifié par rapport au mot de passe par défaut et était inconnu, ce qui suscitait des inquiétudes quant à la nécessité d'une réinitialisation complète en usine (réimage) pour restaurer l'accès et les informations d'identification par défaut. Des questions précises ont été soulevées au sujet de la procédure appropriée pour traiter cette situation :

Environnement

- Centre de gestion Firepower géré par Cisco Secure Firewall 1000, 2100 et 3100 FTD

Résolution

La résolution impliquait de tenter d'accéder au périphérique FTD affecté à l'aide des informations d'identification d'administrateur par défaut avant de poursuivre la procédure de réinstallation plus complexe.

1: Avant de commencer, essayez de vous connecter au périphérique FTD concerné à l'aide des informations d'identification d'administration par défaut.

```
Username: admin
Password: Admin123
```

Cette étape doit être effectuée en premier, car elle pourrait éliminer le besoin de procédures de

récupération plus perturbatrices.

2: Si les informations d'identification par défaut sont exclues, réinitialisez le mot de passe admin à une nouvelle valeur connue via la procédure de modification de mot de passe CLI FTD standard.

Processus de réinstallation : Guide de réinstallation de Cisco Secure Firewall ASA et Threat Defense

- Effectuez une réimage complète du périphérique FTD affecté, en respectant les étapes de la documentation Cisco.
- Restaurez les informations d'identification par défaut via le processus de réinstallation.

Motif

La cause principale était que le mot de passe d'administration sur le périphérique FTD affecté n'avait jamais été modifié par rapport à la valeur par défaut d'usine lors du déploiement initial. La perte d'accès est due à l'hypothèse incorrecte que le mot de passe était inconnu, plutôt qu'à une perte d'informations d'identification réelle. Le périphérique est resté accessible en utilisant les identifiants d'administration par défaut tout au long de l'incident.

Autres informations utiles

- Remplacement de l'unité défectueuse dans le pare-feu sécurisé Défense contre les menaces de haute disponibilité
- Guide de dépannage de Cisco FXOS pour la défense pare-feu : Gestion des images
- Guide de réinstallation de Cisco Secure Firewall ASA et Threat Defense
- Configuration, vérification et dépannage de l'enregistrement des périphériques Firepower
- Configurer la haute disponibilité FTD sur les appareils Firepower
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.